网络分析在网络运维中的应用

摘　要：网络分析就是通过对网络数据的全面监控分析，对网络中传输的数据包进行解码、检测、分析、诊断，排除各种网络应用行为造成的网络故障和问题，准确并快速地定位网络病症，规避网络安全风险，提高网络性能，增强网络可用性。本文介绍了网络分析的位置、数据的筛选、统计方法、分析方法，使用网络分析解决性能评价、网络资源管理和决策，以及识别网络中的安全威胁等进行了详细阐述，通过实例讲解网络分析在实践中的重要作用。

关键词：网络分析；网络故障；网络安全；统计分析
中图分类号：TP311　　文献标识码：A
文章编号：1671-0134（2018）10-061-02　　DOI：10.19483/j.cnki.11-4653/n.2018.10.020

文 / 刘晨光

chinaXiv:202310.01870v1

引言

网络是信息化的基础，是网络业务的高速路，网络本身的稳定性、通畅性决定了网络业务的发展。网络普及率不断提高，人类在执行各种活动的时候越来越依赖网络。不断更新的应用，规模庞大，结构复杂，面临的网络故障越来越复杂，故障处理时间越来越紧张。如何快速定位，如何进行网络溯源，是每个网络运维人员的重要职责。

在实际网络中，通常部署了大量的设备，如交换机、路由器、防火墙、VPN、均衡负载设备、各种终端、服务器等，这些设备上出现的应用故障，都会对业务造成影响。网络分析就是通过对网络数据的全面监控分析，对网络中传输的数据包进行解码、检测、分析、诊断，排除各种网络应用行为造成的网络故障和问题，准确并快速地定位网络病症，规避网络安全风险，提高网络性能，增强网络可用性价值。

1. 网络运维工作中常见的故障

根据网络故障的性质可以分为物理故障与逻辑故障。

（1）物理故障是指设备或线路损坏、插头松动、网络插头误接、线路电磁干扰等故障。

（2）逻辑故障包括配置错误、服务进程或端口异常，以及系统的负载过高、恶意攻击等。

2. 网络故障判断

作为一名网络管理员，在用户反映网络故障时一般会按照自下而上的顺序逐层排除故障。

（1）物理层：网络线缆的通断，交换机端口连通并UP。

（2）数据链路层：ARP 解析是否正常。

（3）网络层：IP 地址是否能 ping 通。

（4）传输层：网络上的服务能否启用，服务端口能否连通。

应用层：应用程序是否正常工作，用户是否能正常使用。

3. 网络分析排查故障

针对网络中一些常见的故障，如网络连通性问题，通过简单的 ping，tracert 命令就可以判断。但遇到一些复杂的情况，间歇性网络故障，应用时断时通、网络速度慢等复杂情况，其原因包括局域网内设备的问题、广域网上链路问题、应用服务器或客户端主机问题、应用软件自身问题等，这就得用网络分析。

（1）网络分析的位置。网络抓包分析的位置，取决于网络拓扑图中数据源和目的服务器，以及路由途径的网络设备。我曾经遇到一个故障，用户总反映 DNS 解析慢，部分域名解析不成功的现象。我们首先在用户端抓包，确实有一部分 DNS 域名一直没有回复，然后在 DNS 服务器端抓包，发现所有收到的解析请求，服务器都解析并响应了。接下来在途径的网络设备上通过端口镜像等方法抓包分析，最后在一个防火墙内口和外口的包对比时，发现数据包数量有差异，这就意味着部分包被防火墙丢弃，然后对这些被丢弃的包进行分析对比，发现被丢掉的都是 DNS 大包，可见防火墙的 MTU 太小，会丢弃大包，修改 DNS 包为最小化或者修改防火墙 MTU 后，问题得到解决。这就是网络分析位置的选取，根据网络拓扑和异常数据流向设置多个数据监控点，逐个排除。

（2）网络分析的数据筛选。网络上有海量的数据包，如何从这些数据中筛选出需要的部分，减少数据分析的工作量，也是数据分析的重要步骤。数据的筛选，可以在抓包之前只抓取有用的数据，这适用于对故障有较清晰的认识，比如上面那个 DNS 丢包的问题，就可以限定只抓源地址、目的地址、协议 DNS 的数据包。也可以在获取所有故障时间段的数据后再进一步筛选，该情况适合于安装了旁路日志系统或者分析系统的情况。一般的筛选条件有限定源地址和目的地址、限定网卡、限定协议，限定服务端口、限定交换机端口等。

ChinaXiv合作期刊

chinaXiv:202310.01870v1

（3）通过对比的方法定位故障。将正常时期的数据与故障时的数据对比，分析找到不同点。有用户称在 C/S 模式登录应用系统时，经常登不上去，我们抓取一段时间的数据，对比这个传输用户名密码的数据包时，发现成功登录的数据包的大小和失败的数据包大小不一样，由此发现应用程序设计的问题。

（4）通过数据流图的方式分析。用户反映在 A 楼快，B 楼慢，由此怀疑 B 楼的交换机性能或者传输策略。用测速工具测试网络速率，A 楼 B 楼速率一样。在用户端抓取一个完整的数据交互过程，用流程图列出所有的交互和时间，发现 B 楼数据包有一个大约 10 秒钟的间隔等待，等待一个互联网域名请求超时，而 A 楼的终端没有配置 DNS 服务器，就直接进行到下一步了，这就找到问题的原因了。

（5）通过统计的方法定位故障。这个是最复杂却也是最常用的方法。有一次，用户反映同一网段内用户上网都很慢，对该交换机上的网络总流量及进出流量做出统计发现，带宽利用率达到 80% 左右，瞬时的利用率甚至更高，造成大量的数据包丢失，广播包数量惊人，端口频闪，此时基本可以判定为广播或路由环路故障。统计可以根据多种维度来进行，协议统计可以分析数据包中每种协议类型的占比重情况；对话统计可以分析特定端点间的所有流量；Http 流量统计可以分析网络某个站点的访问情况，还有很多高级网络统计工具。

4. 网络分析解决性能瓶颈

对于一个应用在网络上的传输性能，会受到带宽、延迟、抖动、丢包等参数的影响，找到影响传输性能的瓶颈因素，从而提升传输性能。在国际网络运维中，用户反映备份线路启用后，网络明显变慢，因此申请增加备线的网络带宽。但通过网络统计分析发现，备线的带宽并没有被占满，还有很大的余量。在客户端和服务器端抓包分析 TCP 协议的交互，耗时大部分发生在服务器端等待客户端的 ACK 确认，但客户端也及时回应了 ACK 报文，问题出在了备线的时延上，因为备线经过迂回线路，时延大概是主线的 2 倍。在这种情况下，单纯增加带宽是解决不了问题的，在当前链路情况下，使用并发连接的应用程序，修改操作系统 TCP 窗口大小，都会使得性能得到明显改观。

5. 资源统计、管理、决策等

通过抓取一段时间网络流量的原始数据，进行网络行为规律及运行趋势分析，可以为网络性能优化、新业务部署、带宽规划、安全策略等决策提供科学的依据。

6. 网络安全分析

通过对数据包的网络行为分析，进行深度网络通讯检测，可以快速发现网络攻击、主动外联、木马通讯、隐蔽信道、异常 DNS 解析、违规操作等危害网络安全的异常行为。要想识别网络上的恶意流量攻击，需要将网络正常时的流量特征了如指掌，进而快速发现异常流量，比如 ARP、TCP、DNS、特定 IP 和端口号等突发流量。有一次，大量用户反映网络变慢、卡顿。通过抓包软件发现网络上几个 IP，尝试与局域网内所有主机建立连接，连接的端口一致且连接之间相隔时间短，流量占用较大，而且这些数据包的源 IP 隶属于同一网段，这极有可能是感染了蠕虫病毒的主机在扫描网络。同样可以通过 TCPSYN 扫描、DOS 攻击等也可以通过异常流量分析找到症结。

结语

以上是日常网络运维中的网络故障以及解决方法，通过实例介绍网络分析的应用，单纯的网络抓包，会捕获大量的数据，而通过各种网络分析的筛选和多种统计方法，多层网络协议分析，可以尽快找出网络中存在的异常。当前，网络分析领域有很多工具，有 wireshark、sniffer、NetFlow、Jflow、Sflow、Syslog、xlog 和 httpwatch、tcpdump、OmniPeak 等，只要能解决问题，都是好的网络分析工具。

网络分析在网络故障处理中发挥着越来越重要的作用，一切网络分析最终依赖的是网络技术人员的知识、经验和分析能力。媒

参考文献

[1]（以色列）Yoram Orzach 著，古宏霞，孙余强译 .Wireshark 网络分析实战 [J]. 人民邮电出版社 .

[2]（美）KevinR.Fall，W.RichardStevens 著，吴英，张玉，许昱玮 译 .《TCP/IP 详解卷一：协议》，机械工业出版社 .

[3] 杨萍，田建春 .Wireshark 网络安全风险评估关键技术研究 [J]. 网络安全技术与应用，2015（09）.

[4] 杨嵘，张国清，韦卫，李仰耀 . 基于 NetFlow 流量分析的网络攻击行为发现 [J]. 计算机工程，2005，31（13）.

[5] 帅亮 .HTTP 流量特征分析与产生 [J]. 中国科学院计算技术研究所，2009.

[6] 魏评 . 基于端口镜像的 OmniPeek 网络协议分析 [J]. 电脑知识与技术，2009，5（04）.

（作者单位：新华社技术局）